PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-304293
(43)Date of publication of application : 24.10.2003

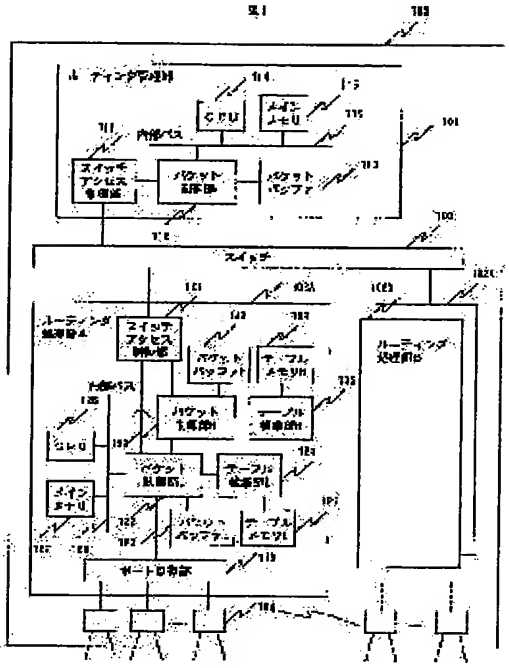
(51)Int.Cl. H04L 12/66

(21)Application number : 2002-107281
(22)Date of filing : 10.04.2002

(71)Applicant : HITACHI LTD
(72)Inventor : MURAKAMI TOSHIHIKO

(54) PACKET REPEATER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method allowing high-speed packet processing even if the high-layer packet processing is performed in a packet repeater, such as a router, a layer 2-3 switch.
SOLUTION: In the packet repeater, such as the router, the layer 2-3 switch, the multilayer high-speed packet processing method is applied to a packet which is decided to perform relay by layer 2 and 3 routing and low-layer packet filtering by means of a conventional ASIC (Application-Specific Integrated Circuit). Additionally, packet repeating processing is performed by preparing a plurality of high-layer filtering functions by means of the ASIC or a network processor according to the analyzing contents of every layer or the packet.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－304293
（P2003－304293A）
(43)公開日　平成15年10月24日(2003.10.24)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ　５Ｋ０３０

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

(21)出願番号　特願2002－107281(P2002－107281)

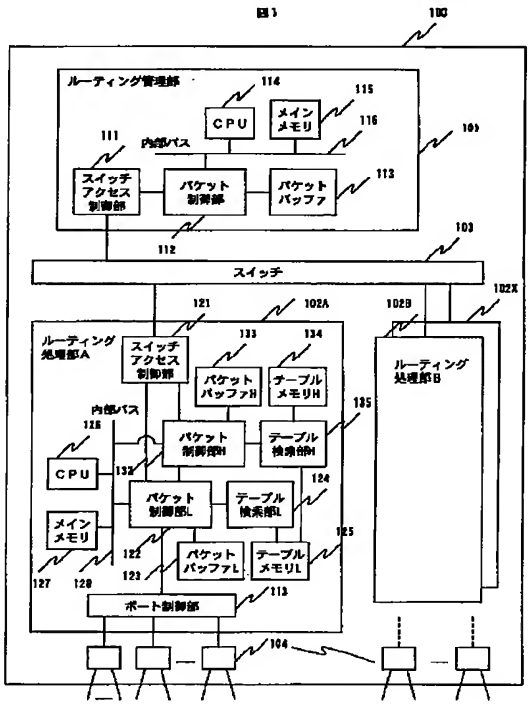
(22)出願日　平成14年４月10日(2002.4.10)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　村上　俊彦
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

Ｆターム(参考)　5K030 GA03 GA15 HA08 HD03 HD05
KA05 KA15 KX24 LB05 LC15
LD19 LE09 MD08

(54)【発明の名称】　パケット中継装置

(57)【要約】
【課題】ルータやレイヤ２－３スイッチのようなパケット中継装置において、高レイヤのパケット処理を行う場合でも高速なパケット処理ができる方法を提供する。
【解決手段】ルータやレイヤ２－３スイッチのようなパケット中継装置において、従来からあるＡＳＩＣによるレイヤ２と３のルーティングおよび低レイヤのパケットのフィルタリングで中継することが決定されたパケットに対して、さらにＡＳＩＣやネットワークプロセッサによる高レイヤのフィルタリング機能をレイヤ毎やパケットの解析内容に応じて複数用意してパケット中継処理を行い、マルチレイヤでの高速パケット処理方法を提供する。



1

【特許請求の範囲】

【請求項１】バケット中継装置において、

レイヤ２およびレイヤ３のバケットを中継する第一の中継手段およびレイヤ２からレイヤ３または４までのレイヤの情報に基づきバケットの中継あるいは廃棄の判定をする第一のフィルタリング手段と、前記第一のフィルタリング手段で中継と決定されたバケットのレイヤ４または５からレイヤ７までのレイヤの任意の範囲の情報に基づきバケット中継あるいは廃棄の判定および中継するバケットの宛先を決定する第二のフィルタリング手段と、バケットを中継する第二の中継手段を備えることを特徴とするバケット中継装置。

【請求項２】請求項１に記載のバケット中継装置であって、

レイヤ２およびレイヤ３の経路制御プロトコルにより経路情報を収集し、ルーティングテーブルの作成および更新を行い、レイヤ２からレイヤ３または４までの情報に基づいてバケットのフィルタリングを行うための第一のフィルタリングテーブルと、レイヤ４または５からレイヤ７までの情報に基づいてバケットの宛先となる情報を決定する、またはフィルタリングを行うための第二のフィルタリングテーブルを作成するルーティング管理部と、

前記ルーティング管理部から配布された前記ルーティングテーブルの内容によりバケットの中継処理を行う第一のバケット中継処理部と、

前記ルーティング管理部から配布された前記第一のフィルタリングテーブルの内容によりバケットのフィルタリングを行う第一のフィルタリング処理部と、

前記第一のフィルタリング処理部により中継することが決定されたバケットについて前記ルーティング管理部から配布された前記第二のフィルタリングテーブルの内容により宛先となる情報を決定する、またはフィルタリングを行う第二のフィルタリング処理部と、

前記第二のフィルタリング処理部により中継することが決定され、それと同時に前記第二のフィルタリングテーブルの情報に基づいてバケットの変換を行い、バケットの中継を行う第二のバケット中継処理部とを、複数有するルーティング処理部が、内部通信線を介して複数接続されることを特徴とするバケット中継装置。

【請求項３】請求項１または２に記載のバケット中継装置であって、

サーバ装置群をエンドユーザからは仮想的に一つのサーバ装置として見えるようにする場合に、当該バケット中継装置が前記サーバ装置群の入口とした場合に、入力側となった前記ルーティング処理部で前記サーバ装置群に対してバケットを中継する手段を備えることを特徴とするバケット中継装置。

【請求項４】請求項１または２に記載のバケット中継装置であって、

2

サーバ装置群をエンドユーザからは仮想的に一つのサーバ装置として見えるようにする場合に、当該バケット中継装置が前記サーバ装置群の入口とした場合に、出力側となった前記ルーティング処理部で前記サーバ装置群に対してバケットを中継する手段を備えることを特徴とするバケット中継装置。

【請求項５】請求項１または２に記載のバケット中継装置であって、

前記バケット中継装置が宛先となるバケットに対して、前記ルーティング処理部が前記ルーティング管理部へのバケットであると判断した場合、前記ルーティング処理部内の前記第一のフィルタリング処理部または第二のフィルタリング処理部により、所定の前記バケットを廃棄する手段を備えることを特徴とするバケット中継装置。

【請求項６】請求項１または２に記載のバケット中継装置であって、

前記バケット中継装置が宛先となるバケットが、前記ルーティング処理部により前記ルーティング管理部へ中継された場合に、前記ルーティング管理部が前記第一のフィルタリング手段および前記第二のフィルタリング手段を有して、所定の前記バケットを廃棄する手段を備えることを特徴とするバケット中継装置。

【請求項７】請求項１または２に記載のバケット中継装置であって、

前記第一または第二のフィルタリングテーブルは、バケットのレイヤ毎のヘッダ情報またはインフォメーション部の情報を設定する条件フィールドと、その条件にマッチした場合に該当バケットを変換せずに中継する、変換して中継する、廃棄するか等を指示する第一の指示フィールドと、前記第一の指示フィールドで変換して中継すると指示された場合に、変換の方法を指示する第二の指示フィールドを有することを特徴とするバケット中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はバケット中継装置のマルチレイヤのバケット処理方法に関する。

【０００２】

【従来の技術】従来の技術では、バケット中継装置であるルータやレイヤ２－３スイッチのバケット中継において、レイヤ４まではハードウェアでバケットのヘッダ情報等により中継やフィルタリングを行うことができる。レイヤ５以上になると、ＳＳＬ（Secure Socket Layer）セッションＩＤやＵＲＬ（Uniform Resource Locator）というような識別子のように想定可能なアプリケーションのバケットに対してはハードウェアでバケット処理をアシスト可能であるが、その他のバケットに対してはソフトウェアによりバケットを処理している。

【０００３】従来の技術では、ハードウェアによるアシスト機能が限定され、ソフトウェアによる中継処理もＣ

ＰＵ処理性能によって上限が抑えられるという問題がある。

【０００４】

【発明が解決しようとする課題】従来の技術では、すべてのレイヤでそのヘッダ情報等を見て高速にパケット中継やフィルタリングを実行するためには、ＡＳＩＣ（Application Specific Integrated Circuit）やネットワークプロセッサによるパケット処理が必要となるが、上位レイヤになるほどパケットのヘッダ部やインフォメーション部の情報量が増え、セッション数等の管理する情報も増える。そのため、ＡＳＩＣではある範囲の部分でしかアシストはできず、またネットワークプロセッサでも、プログラム規模が大きくなりネットワークプロセッサのプログラムメモリ内に入らないといった問題が発生する。

【０００５】本発明の目的は、ルータやレイヤ２－３スイッチのようなパケット中継装置において、高レイヤのパケット処理を行う場合でも高速なパケット処理ができる方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明は、ルータやレイヤ２－３スイッチのようなパケット中継装置において、ＡＳＩＣによる低レイヤのパケットのフィルタリングの後に高レイヤのパケット処理を行うＡＳＩＣやネットワークプロセッサをレイヤ毎やパケットの解析範囲に応じて１つまたは複数用意して、マルチレイヤでの高速パケット処理方法を提供する。

【０００７】

【発明の実施の形態】本発明の第一の実施の形態を図１から図１０を参照して説明する。

【０００８】図１は本実施形態を適用するパケット中継装置の構成例を示す図である。パケット中継装置１００は、レイヤ２およびレイヤ３の経路制御プロトコルにより経路情報を収集し、ルーティングテーブルの作成および更新を行い、そしてネットワーク管理者によりパケットのフィルタリングの設定を行うルーティング管理部１０１と、ルーティング管理部１０１から配布されたルーティングテーブルやフィルタリングテーブルに基づき、パケットのルーティング処理を行う複数のルーティング処理部１０２（１０２Ａ、１０２Ｂないし１０２Ｘ）と、ルーティング管理部１０１と複数のルーティング処理部１０２を接続するスイッチ等の内部通信線１０３と回線インタフェース１０４を有する。

【０００９】ルーティング管理部１０１は、ＣＰＵ１１４、メインメモリ１１５、内部通信線１１６を介してパケットの送受信を制御するパケット制御部１１２を有する。またパケット制御部１１２に接続するパケットバッファ１１３を有する。パケット制御部１１２はスイッチアクセス制御部１１１により内部通信線１０３と接続される。

【００１０】ルーティング処理部１０２は、ＣＰＵ１２６、メインメモリ１２７、レイヤ２および３のルーティングとレイヤ２から４のフィルタリングを行うパケット制御部“Ｌ”１２２、レイヤ５から７のフィルタリングを行うパケット制御部“Ｈ”１３２を有しこれらが内部バス等の内部通信線１２８で接続されている。パケット制御部“Ｌ”１２２とパケット制御部“Ｈ”１３２は、ＡＳＩＣまたはネットワークプロセッサで構成することが望ましい。

【００１１】パケット制御部“Ｌ”１２２は送受信されるパケットを格納するパケットバッファ“Ｌ”１２３を有し、パケット制御部“Ｈ”１３２は同様にパケットバッファ“Ｈ”１３３を有する。また、パケット制御部“Ｌ”１２２にはレイヤ２およびレイヤ３のルーティングテーブルやレイヤ２からレイヤ４のフィルタリングテーブルを格納するテーブルメモリ“Ｌ”１２５を有して送受信されるパケットのヘッダ等との比較を行うテーブル検索部“Ｌ”１２４が接続される。

【００１２】同様にパケット制御部“Ｈ”１３２にはレイヤ５からレイヤ７のフィルタリングテーブルを格納するテーブルメモリ“Ｈ”１３４を有して送受信されるパケットのヘッダ等との比較を行うテーブル検索部“Ｈ”１３５が接続される。パケット制御部“Ｌ”１２２は１つまたは複数の回線インタフェース１０４を接続するポート制御部１１３と接続され、内部通信線１０３とスイッチアクセス制御部１２１を介して接続される。パケット制御部“Ｈ”１３２はパケット制御部“Ｌ”１２２と接続され、内部通信線１０３とスイッチアクセス制御部１２１を介して接続される。尚、他のルーティング処理部１０２Ｂないし１０２Ｘも同様の構成を有する。

【００１３】図１のパケット中継装置の構成例は、パケットのレイヤ２から７までの情報をパケット制御部を２つ用意して、１つめのパケット制御部“Ｌ”１２２でレイヤ２からレイヤ４までのフィルタリングを行い、２つめのパケット制御部“Ｈ”１３２でレイヤ５から７のフィルタリングを行う例を示しているが、この例に限定されず、パケット制御部をレイヤ毎やパケットの解析内容に応じて複数用意することも可能である。

【００１４】以下では、まずＷＥＢ等のサーバへの一般的なアクセスの方法や、レイヤ４－７スイッチを用いた場合のアクセスの方法を説明し、その次に本実施形態を適用するパケット中継装置を使用した場合のネットワーク構成の一例および処理概要について説明する。

【００１５】図２はインターネットでＷＥＢサーバをアクセスする際に利用されるＨＴＴＰ（Hyper Text Transport Protocol）のパケットの例を示す図である。ＨＴＴＰメッセージ２１０は、リクエストやレスポンス等の情報を示すＨＴＴＰヘッダ２１１と、ＨＴＴＰボディ２１２から構成される。ＬＡＮ環境でＨＴＴＰメッセージ２１０は、ＭＡＣ（Media Access Control）ヘッダ２２

１と、ＩＰ（InternetProtocol）ヘッダ２２２と、ＴＣＰ（Transmission Control Protocol）ヘッダ２２３を付加されたＨＴＴＰパケット２２０として構成される。

【００１６】また、セキュリティを考慮してＳＳＬ（Secure Socket Layer）を使用した場合、ＨＴＴＰメッセージ２１０は暗号化されたＨＴＴＰメッセージ２３５となり、ＳＳＬヘッダ２３４が付加されたＨＴＴＰパケット２３０として構成される。それぞれのデータの概要については、ＭＡＣヘッダ２２１のＴＹＰＥフィールドが０ｘ０８００（１６進数）の場合はその上位のプロトコルがＩＰであることを示し、ＩＰヘッダ２２２のＰＲＯＴＯＣＯＬフィールドが６の場合はその上位のプロトコルがＴＣＰであることを示し、ＴＣＰヘッダ２２３の宛先ポート番号が８０である場合はその上位のプロトコルがＨＴＴＰであることを示し、またＴＣＰヘッダ２２３の宛先ポート番号が４４３である場合はその上位のプロトコルがＳＳＬを利用したＨＴＴＰであることを示している。

【００１７】図３はクライアントがインターネットやＬＡＮのようなネットワークを介して、ＷＥＢサーバやＦＴＰ（File Transfer Protocol）サーバを利用する場合のネットワーク構成の一例を示す図である。端末３０１ＡがＷＥＢサーバ３０２Ａをアクセスする場合、まずネットワーク３００内のＤＮＳ（Domain Name Server）３０４とのメッセージのやりとり３０５Ａにより、ＷＥＢサーバ３０２Ａのホスト名からＩＰアドレスを取得し、このＩＰアドレスを宛先とするＨＴＴＰのリクエストメッセージ３０６ＡがＷＥＢサーバ３０２Ａに送信される。ＷＥＢサーバ３０２Ａは、ＨＴＴＰのリクエストメッセージ３０６Ａのリクエスト内容に応じたＨＴＴＰのレスポンスメッセージ３０７Ａを端末３０１Ａに送信する。

【００１８】ＨＴＴＰのレスポンスメッセージ３０７Ａの宛先アドレスはリクエストメッセージ３０６Ａの送信元ＩＰアドレスが用いられるため、ＤＮＳ３０４は使用されない。ＤＮＳ３０４はホスト名とＩＰアドレスの対応を管理しており、このネットワーク構成の例では一つしか示していないが、ドメインが複数存在する場合にはドメインを管理する範囲に応じて複数存在することもあり、複数のＤＮＳ間で連携してホスト名とＩＰアドレスの対応を管理する。端末３０１ＢがＷＥＢサーバ３０２Ｃをアクセスする場合、端末３０１ＣがＦＴＰサーバ３０３Ｂをアクセスする場合も、前記と同様なメッセージのやりとりが行われる。ただし、ＦＴＰサーバ３０３をアクセスする場合には、ＨＴＴＰメッセージを用いる場合と、ＦＴＰプロトコルを利用する場合がある。

【００１９】図４はクライアントがインターネットやＬＡＮのようなネットワークを介して、ＷＥＢサーバやＦＴＰサーバを利用する際に、レイヤ４－７スイッチを用いている場合のネットワーク構成の一例を示す図である。ＷＥＢサーバ４０２Ａないし４０２Ｃはレイヤ４－７スイッチ４０６Ａにより仮想ホスト名４０２Ｇとして管理され、ＦＴＰサーバ４０３Ａないし４０３Ｃはレイヤ４－７スイッチ４０６Ｂにより仮想ホスト名４０３Ｇとして管理されているものとし、クライアントが仮想ホスト名でサーバをアクセスするために、レイヤ４－７スイッチ４０６とＤＮＳ３０４は情報の交換を行っているものとする。

【００２０】端末４０１ＡがＷＥＢサーバ４０２Ｇをアクセスする場合、図３での説明と同様にＤＮＳ３０４とのやりとりの後、ＨＴＴＰのリクエストメッセージ４０７ＡがＷＥＢサーバ４０２Ｇに送信される。その際、レイヤ４－７スイッチ４０６ＡがＨＴＴＰのリクエストメッセージ４０７Ａの内容やＷＥＢサーバ４０２Ａないし４０２Ｃの稼動状況により、適切なＷＥＢサーバへとＨＴＴＰのリクエストメッセージを振り分ける。この例では、ＨＴＴＰのリクエストメッセージ４０７Ａは、４０８ＡとしてＷＥＢサーバ４０２Ａに送信されるものとしている。

【００２１】ＨＴＴＰのリクエストメッセージ４０７Ａは、図２で示したようにＳＳＬを使用している場合は、暗号化された内容をレイヤ４－７スイッチ４０６Ａが暗号をデコードしてＨＴＴＰのリクエストメッセージ４０８Ａでは復号化する場合もある。ＷＥＢサーバ４０２Ａは、ＨＴＴＰのレスポンスメッセージ４０９Ａを端末４０１Ａを送信する。その際に前記のように、レイヤ４－７スイッチ４０６Ａが暗号化されていないＨＴＴＰのレスポンスメッセージ４０９Ａを暗号化してＨＴＴＰのレスポンスメッセージ４１０Ａとして送信する場合もある。端末４０１ＢがＷＥＢサーバ４０２Ｇをアクセスする場合、端末４０１ＣがＦＴＰサーバ４０３Ｇをアクセスする場合も、前記と同様なメッセージのやりとりが行われる。ただし、サーバ側からクライアント側へのメッセージは、４０９Ｂや４０９Ｃのようにレイヤ４－７スイッチ４０６Ａや４０６Ｂを介さない場合もある。

【００２２】図５は本実施形態を適用するパケット中継装置１００を用いたネットワーク構成の一例を示す図である。パケット中継装置１００、端末５０１、ＷＥＢサーバ５０２、ＦＴＰサーバ５０３、ＤＮＳ３０４が、ネットワーク６１０ないし６７０を介して接続される。パケット中継装置１００は、レイヤ２およびレイヤ３のルーティング処理を行い、かつ、図４で示したレイヤ４－７スイッチ４０６と同様に適切なＷＥＢサーバやＦＴＰサーバへとＨＴＴＰのメッセージを振り分ける。レイヤ４－７スイッチとの違いは、同一のネットワーク上にないＷＥＢサーバ５０２Ａないし５０２Ｃをパケット中継装置１００Ａにより仮想ホスト名５０２Ｇでアクセスできるようにすることや、ＦＴＰサーバ５０３Ａないし５０３Ｃをパケット中継装置１００Ｂにより仮想ホスト名５０３Ｇでアクセスできるようにすることである。

【００２３】図６は図５で示されるネットワークやパケット中継装置、端末等に割り当てられているＩＰアドレスの一例を示す図である。図７（ａ）はパケット中継装置１００Ａのテーブルメモリ“Ｌ”１２５に格納されるルーティングテーブル７００Ａの一例を示す図であり、図７（ｂ）は中継装置１００Ｂのテーブルメモリ“Ｌ”１２５に格納されるルーティングテーブル７００Ｂの一例を示す図である。ルーティングテーブル７００は、ネットワークアドレス７０１、ネクストホップアドレス７０２、および出力ポート７０３を一組とするエントリ７０４を複数格納する構成となっている。

【００２４】図８はパケット中継装置１００のテーブルメモリ“Ｌ”１２５に格納されるフィルタリングテーブル“Ｌ”８００の一例を示す図である。フィルタリングテーブル“Ｌ”８００は、レイヤ２から４までのマッチ条件８０１、マッチしたときの処理８０２、およびパケット制御部“Ｈ”１３２に転送したときに使用する処理ＩＤ８０３を一組とするエントリを複数格納する（８０４、８０５、８０６等）構成となっている。図９はパケット中継装置１００のテーブルメモリ“Ｈ”１３４に格納されるフィルタリングテーブル“Ｈ”９００の一例を示す図である。フィルタリングテーブル“Ｈ”９００は、図８で示した処理ＩＤ８０３をキーとして検索するための処理ＩＤ９０１、レイヤ５から７までのマッチ条件９０２、およびマッチしたときの処理９０３を一組とするエントリを複数格納する（９０４、９０５、９０６等）構成となっている。

【００２５】図１０はルーティング処理部１０２がパケットを受信してからパケットを内部通信線１０３、またはポート制御部１１３へパケットを送信するまでの処理手順の一例を示す図である。図５において、端末５０１ＡおよびＢがＷＥＢサーバ５０２Ｇをアクセスする場合、パケット中継装置１００Ａは端末５０１Ａからのパケットを受信すると（ステップ１０１１）、まずパケット処理“Ｌ”１０１０を行う。パケット処理“Ｌ”１０１０においては、パケット受信（ステップ１０１２）と同時にパケットのレイヤ２、３、４のヘッダ解析を行い（ステップ１０１３）、ルーティングテーブル７００Ａの検索を行う（ステップ１０１４）。

【００２６】受信したパケットの宛先アドレスは192.168.30.30であるので、エントリ７０５がマッチして、ネットワークアドレスは192.168.30.0、ネクストホップアドレスは192.168.30.1、出力ポートはPA2であることがわかる。さらに、フィルタリングテーブル“Ｌ”８００の検索を行い、エントリ８０４がマッチして、パケット制御部“Ｈ”へ転送することになり、転送パケットの作成を行い（ステップ１０１５）、処理ＩＤ８０３が「００１」であるという情報を渡して、パケット処理“Ｈ”１０２０を行う。

【００２７】その他の受信パケットについては、ルーティングテーブル７００に宛先がない場合や、フィルタリングテーブル８００で条件がマッチして廃棄となっている場合は、そのパケットは廃棄される（ステップ１０１５）。ルーティングテーブル７００に宛先が存在して、フィルタリングテーブル８００にマッチする条件がない場合は、そのパケットはパケット送信処理を行う（ステップ１０３０）。レイヤ２、３，４のヘッダ解析を行って（ステップ１０１３）、ＩＰヘッダやＴＣＰヘッダにオプションヘッダが設定されている場合等は、ソフトウェア処理を行う（ステップ１０４０）。

【００２８】パケット処理“Ｈ”１０２０においては、パケット受信（ステップ１０２１）と同時にパケットのレイヤ５以上のヘッダ解析を行い（ステップ１０２２）、フィルタリングテーブル“Ｈ”９００の検索を行う（ステップ１０２３）。パケット処理“Ｌ”１０１０から渡された処理ＩＤを元に、フィルタリングテーブル“Ｈ”９００の処理ＩＤ９０１が「００１」の中から、エントリ９０４がマッチした場合、ＩＰヘッダのＤＡを192.168.30.10に設定することになり、再度ルーティングテーブル７００Ａの検索を行い、ネクストホップアドレスと出力ポートは変化せずに、転送パケットの作成を行い（ステップ１０２４）、パケット送信処理を行う（ステップ１０３０）。この時の端末５０１ＡからＷＥＢサーバ５０２Ｇへのパケットの流れは、図５の５０４Ａのようになる。前記ステップ１０２３において、受信したパケットは端末５０１Ｂからのものとして、フィルタリングテーブル“Ｈ”９００の処理ＩＤ９０１が「００１」の中から、エントリ９０５がマッチした場合、ＩＰヘッダのＤＡを192.168.40.10に設定することになり、再度ルーティングテーブル７００Ａの検索を行い、ネクストホップアドレスと出力ポートは、エントリ７０６のように変化して、転送パケットの作成を行い（ステップ１０２４）、パケット送信処理を行う（ステップ１０３０）。

【００２９】この時の端末５０１ＢからＷＥＢサーバ５０２Ｇへのパケットの流れは、図５の５０４Ｂのようになる。端末５０１ＣがＦＴＰサーバ５０３Ｇをアクセスする場合、パケット中継装置１００は前記と同様の処理を行う。この場合、フィルタリングテーブル“Ｌ”８００ではエントリ８０６がマッチし、フィルタリングテーブル“Ｈ”ではエントリ９０６がマッチして、レイヤ５以上の内容については不問で、ＦＴＰサーバ５０３Ｇの実際のＦＴＰサーバ５０３Ａないし５０３Ｃの中で、この時点で負荷の一番低いＦＴＰサーバ５０３Ｂのアドレス192.168.50.10をＩＰヘッダのＤＡに設定し、再度ルーティングテーブル７００Ａの検索を行い、ネクストホップアドレスと出力ポートは変化せずに、転送パケットの作成を行い（ステップ１０２４）、パケット転送処理を行う（ステップ１０３０）。この時の端末５０１ＣからＦＴＰサーバ５０３Ｇへのパケットの流れは、図５の

５０４Ｃのようになる。

【００３０】第一の実施の形態では、パケット中継装置がレイヤ４－７の情報をもとにサーバをアクセスする場合のサーバ選択の一例を示したが、パケット制御部“Ｌ”１２２でレイヤ２から４のパケット処理、パケット制御部“Ｈ”１３２でレイヤ５から７のパケット処置を行うような様々な例、例えばファイアウォール機能やＱｏＳ（Quality of Service）機能を実現する際にも使用できる。

【００３１】次に本発明の第二の実施形態を図１１と図１２を参照して説明する。第二の実施形態では、第一の実施形態で説明したパケット制御部“Ｈ”１３２の処理を入力側のルーティング処理部１３２で行う場合と、出力側のルーティング処理部１３２で行う場合の処理概要について説明する。

【００３２】図１１はパケット中継装置１００において、ネットワーク１１０１Ａからサーバ１１０２Ａないし１１０２Ｃをアクセスする場合に、入力側のルーティング処理部１０２Ａのパケット制御部“Ｈ”１３２Ａで、第一の実施の形態で説明したようなサーバの選択が行われた場合のパケットの流れを示す図である。

【００３３】通常は１１０３のようなパケットの流れであるとして、パケット制御部“Ｈ”１３２Ａがレイヤ５以上の情報により、サーバ１１０２Ａないし１１０２Ｃを選択するような処理の場合、パケットの流れは途中までは１１０４で、パケット制御部“Ｈ”１３２Ａからは１１０５Ａないし１１０５Ｃのようになる。この場合の出力側のルーティング処理部はどれでも選択できる可能性があるため、サーバ群を広域に配置するのに適しているが、入力側のパケット制御部“Ｈ”１３２Ａの処理負荷が大きくなる可能性がある。

【００３４】図１２はパケット中継装置１００において、ネットワーク１２０１Ａからサーバ１２０２Ａないし１２０２Ｃをアクセスする場合に、出力側のルーティング処理部１３２Ｂのパケット制御部“Ｈ”１３２Ｂで、第一の実施の形態で説明したようなサーバの選択が行われた場合のパケットの流れを示す図である。通常は１２０３のようなパケットの流れであるとして、パケット制御部“Ｈ”１３２Ｂがレイヤ５以上の情報により、サーバ１２０２Ａないし１２０２Ｃを選択するような処理の場合、パケットの流れは途中までは１２０４で、パケット制御部“Ｈ”１３２Ｂからは１２０５Ａないし１２０５Ｃのようになる。この場合の出力側のルーティング処理部は一つしか選択できない可能性があるため、サーバ群をルーティング処理部の配下に配置するのに適している。パケット制御部“Ｌ”１２２Ａによりレイヤ２から４の情報で、出力側のルーティング処理部１０２を複数選択できる場合は、図１２のルーティング処理部１０２Ｂのパケットの流れが他のルーティング処理部でも実施されるような形態となる。

【００３５】次に本発明の第三の実施の形態を図１３と図１４を参照して説明する。第三の実施の形態では、第一の実施の形態で説明したパケット制御部の処理で、パケットの宛先がルーティング管理部宛となった場合として、ＤｏＳ攻撃やＤＤｏＳ（ＤＤｏＳ＝Distributed Denial of Service）攻撃のような悪意のあるパケットを、ルーティング処理部内のパケット制御部で廃棄する場合と、ルーティング管理部内にパケット制御部“Ｈ”を有することにより廃棄する場合の処理概要について説明する。

【００３６】図１３と図１４はパケット中継装置１００のルーティング管理部１０１を宛先とするパケットを受信した場合のパケット中継装置１００の構成の一例とパケットの流れを示す図である。ルーティング管理部１０１宛のパケットには、経路制御プロトコルなどの制御パケットがほとんどであるが、場合によってはパケット中継装置の動作に問題を生じさせるようなパケットである可能性もある。このようなパケットを、図１３ではパケット制御部“Ｌ”１２２Ａとパケット制御部“Ｈ”１３２Ａで、図１４ではパケット制御部１２２Ａとルーティング管理部１０１にレイヤ５から７までのフィルタリングを行うパケット制御部“Ｈ”１４０１を有することで、廃棄できるようにする。

【００３７】ＤｏＳ攻撃の代表的なものとしては、要求されていないＰｉｎｇ応答メッセージやＩＰアドレスが不正なメッセージの大量送信等があるが、これらはパケット制御部“Ｌ”１２２のフィルタリングテーブル８００で廃棄指定が可能である。つまり、レイヤ２から４までの情報により不正なパケットやＤｏＳ攻撃のパケットはフィルタリングテーブル８００の廃棄指定により廃棄できる。

【００３８】しかし、この廃棄指定だけではフィルタリングできないパケット、すなわちレイヤ２から４までの情報だけでは正常なパケットと見える悪意のあるパケットを図１３ではパケット制御部“Ｈ”１３２、図１４ではパケット制御部“Ｈ”１４０１のフィルタリングテーブル９００の廃棄指定で廃棄できるようにする。これにより、例えば、ＨＴＴＰでＷＥＢサーバに存在しないページのリクエストを大量送信して、Ｎｏｔ　Ｆｏｕｎｄのレスポンスメッセージを大量発生させるようなパケットを廃棄できるようになる。

【００３９】また、上記実施形態の応用により、ルータ、レイヤ２－３スイッチ、アプリケーションスイッチ、コンテンツ内容によるスイッチングやロードバランス等、を実現することができる。

【００４０】

【発明の効果】本発明によれば、マルチレイヤでの高速パケット処理を実現できる。

【図面の簡単な説明】

【図１】パケット中継装置の構成例を示す図。

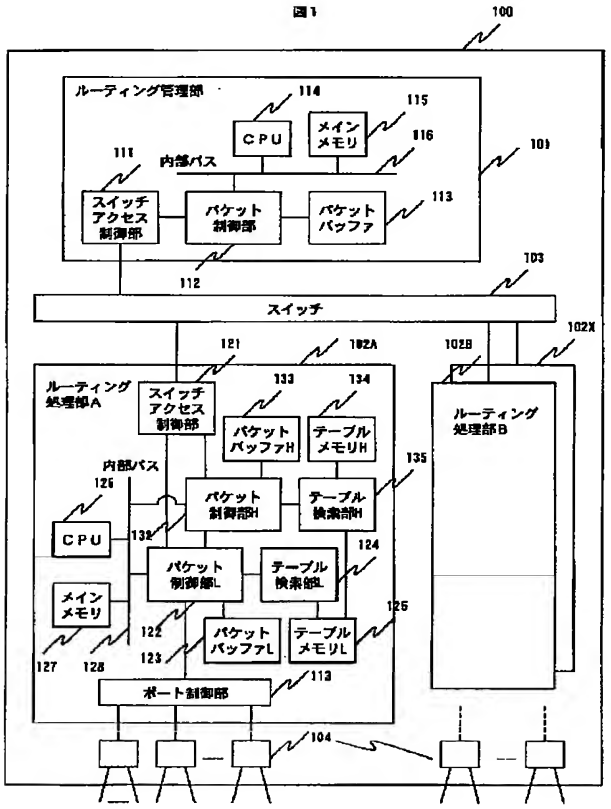
11

【図２】ＨＴＴＰパケットの構成例を示す図。
【図３】サーバをアクセスする例を示す図。
【図４】レイヤ４－７スイッチを使用し、サーバをアクセスする例を示す図。
【図５】パケット中継装置を使用し、サーバをアクセスする例を示す図。
【図６】ネットワークと装置のＩＰアドレスの例を示す図
【図７】ルーティングテーブルの構成例を示す図。
【図８】フィルタリングテーブル“Ｌ”の構成例を示す図。
【図９】フィルタリングテーブル“Ｈ”の構成例を示す図。
【図１０】パケット送受信処理の処理概要を示す図。

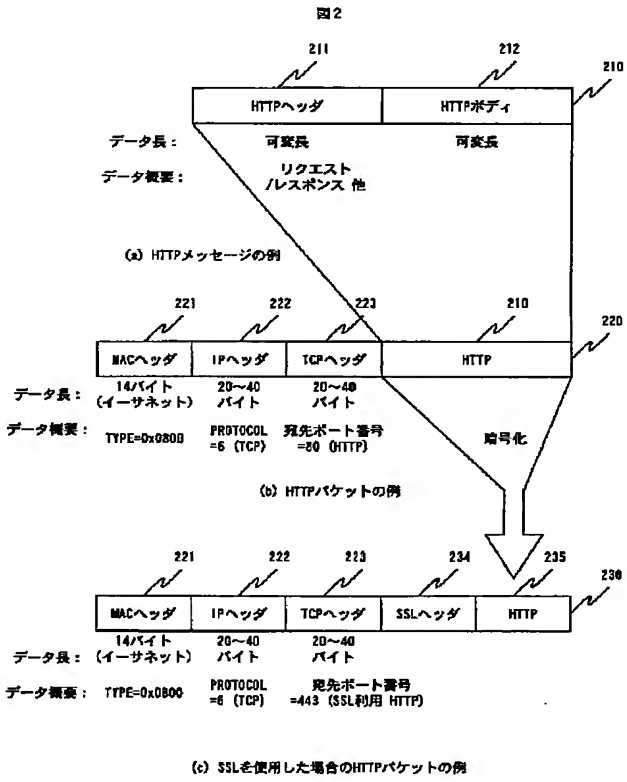
12

＊【図１１】入力側のパケット制御部でサーバ選択を行う例を示す図。
【図１２】出力側のパケット制御部でサーバ選択を行う例を示す図。
【図１３】ルーティング管理部宛のパケットをルーティング処理部内のパケット制御部で廃棄する例を示す図。
【図１４】ルーティング管理部宛のパケットをルーティング管理部内のパケット制御部で廃棄する例を示す図。
【符号の説明】
１００…パケット中継装置
１１２、１２２、１３２、１４０１…パケット制御部
２２０、２３０…ＨＴＴＰパケット
８００…フィルタリングテーブル“Ｌ”
９００…フィルタリングテーブル“Ｈ”

【図１】

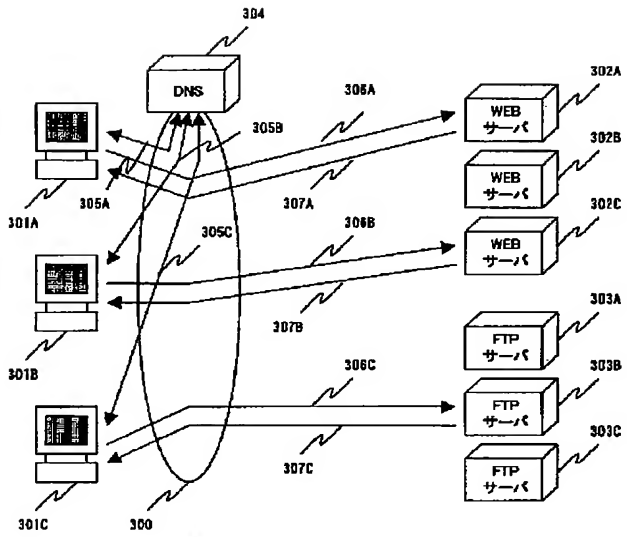


【図２】



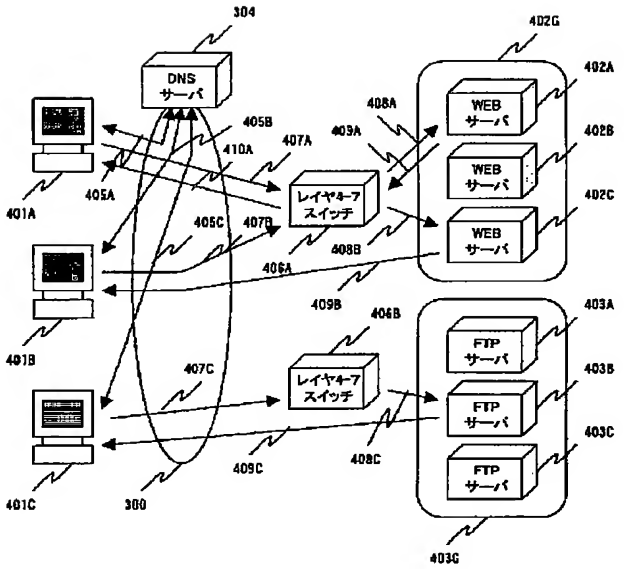
【図３】

図３



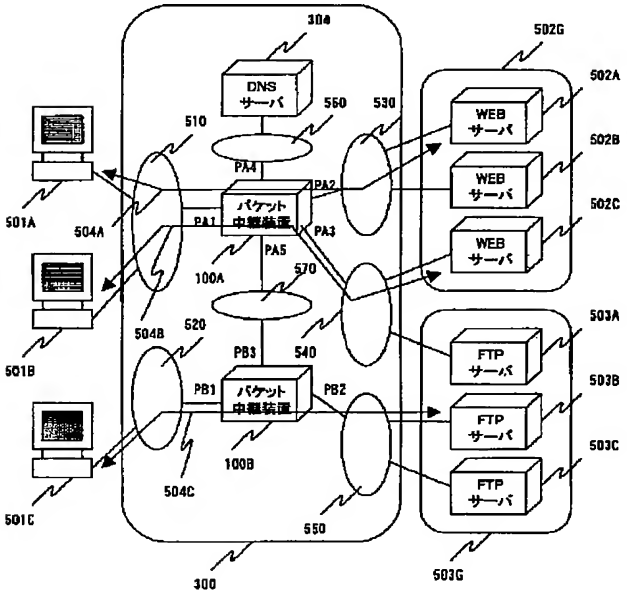
【図４】

図４



【図５】

図５



【図８】

図８

801 マッチ条件	802 処理	803 処理ID
（IPヘッダのDA＝192.168.30.30）AND（TCPヘッダの宛先ポート＝80（HTTP））	パケット制御部Hへ転送	001
IPヘッダのSA＝192.168.30.10	廃棄	
⋮	⋮	
（IPヘッダのDA＝192.168.50.50）AND（TCPヘッダの宛先ポート＝21（FTP））	パケット制御部Hへ転送	002
⋮	⋮	

800　804　805　806

【図９】

図９

901 処理ID	902 マッチ条件	903 処理
001	URL＝www.502.net/index1.htm	IPヘッダのDAを192.168.30.10に設定
001	URL＝www.502.net/index3.htm	IPヘッダのDAを192.168.40.10に設定
⋮	⋮	⋮
002	すべてマッチ	IPヘッダのDAを負荷の一番低いFTPサーバのIPアドレスに設定
	⋮	⋮

900　904　905　906

【図６】

図６（ａ）

ネットワーク/装置	IPアドレス
ネットワーク510	192.168.10.0
ネットワーク520	192.168.20.0
ネットワーク530	192.168.30.0
ネットワーク540	192.168.40.0
ネットワーク550	192.168.50.0
ネットワーク560	192.168.60.0
ネットワーク570	192.168.70.0
パケット中継装置100A ポートPA1	192.168.10.1
パケット中継装置100A ポートPA2	192.168.30.1
パケット中継装置100A ポートPA3	192.168.40.1
パケット中継装置100A ポートPA4	192.168.50.1
パケット中継装置100A ポートPA5	192.168.70.1
パケット中継装置100B ポートPB1	192.168.20.1
パケット中継装置100B ポートPB2	192.168.50.1
パケット中継装置100B ポートPB3	192.168.70.2

600A

図６（ｂ）

ネットワーク/装置	IPアドレス
端末501A	192.168.10.10
端末501B	192.168.10.20
端末501C	192.168.20.10
DNS304	192.168.60.10
WEBサーバ502A	192.168.30.10
WEBサーバ502B	192.168.30.20
WEBサーバ502C	192.168.40.10
WEBサーバ502G	192.168.30.30
WEBサーバ503A	192.168.40.20
WEBサーバ503B	192.168.60.10
WEBサーバ503C	192.168.50.20
WEBサーバ503G	192.168.50.60

600B

【図７】

図７（ａ）

701 ネットワーク	702 ネクストホップ	703 出力ポート
192.168.10.0	192.168.10.1	PA1
192.168.20.0	192.168.70.2	PA5
192.168.30.0	192.168.30.1	PA2
192.168.40.0	192.168.40.1	PA3
192.168.50.0	192.168.70.2	PA5
192.168.60.0	192.168.60.1	PA4
192.168.70.0	192.168.70.1	PA5
⋮	⋮	⋮

704 705 706

700A

図７（ｂ）

701 ネットワーク	702 ネクストホップ	703 出力ポート
192.168.10.0	192.168.70.1	PB3
192.168.20.0	192.168.20.1	PB1
192.168.30.0	192.168.70.1	PB3
192.168.40.0	192.168.70.1	PB3
192.168.50.0	192.168.50.1	PB2
192.168.60.0	192.168.70.1	PB3
192.168.70.0	192.168.70.2	PB3
⋮	⋮	⋮

707

700B

【図１０】

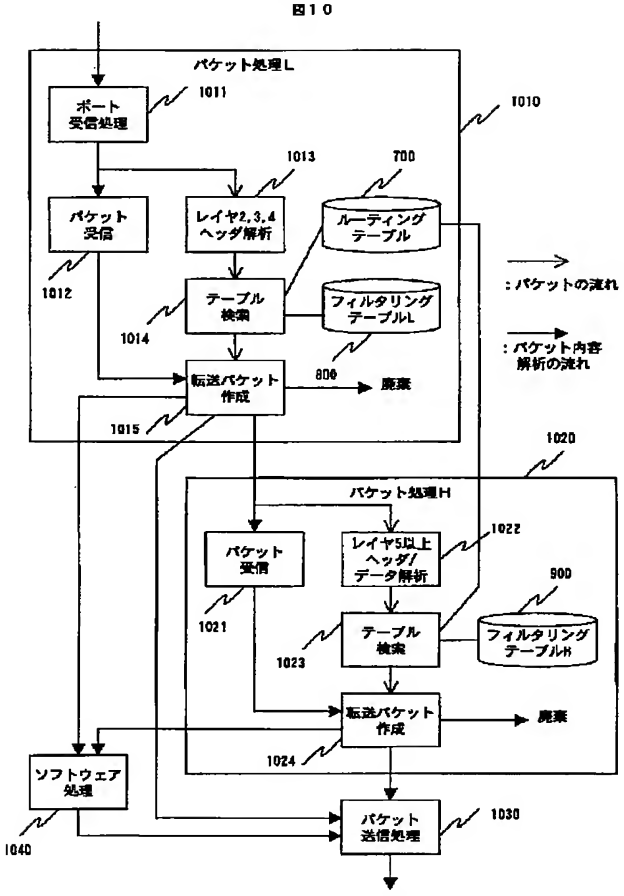


図１０
パケット処理L
ポート受信処理
1011
1010
1013
700
パケット受信
レイヤ2,3,4ヘッダ解析
ルーティングテーブル
1012
テーブル検索
フィルタリングテーブルL
1014
：パケットの流れ
：パケット内容解析の流れ
転送パケット作成
800
廃棄
1015
1020
パケット処理H
パケット受信
レイヤ5以上ヘッダ/データ解析
1022
900
1021
テーブル検索
フィルタリングテーブルH
1023
転送パケット作成
廃棄
1024
ソフトウェア処理
パケット送信処理
1030
1040

【図１１】

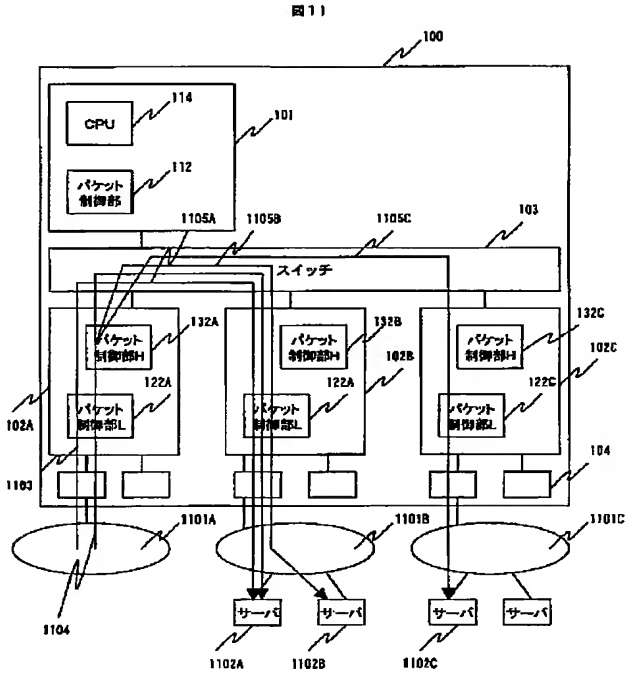


図１１
100
CPU
114
101
パケット制御部
112
1105A
1105B
1105C
103
スイッチ
パケット制御部H
132A
132B
132C
102C
102B
パケット制御部L
122A
122C
102A
1103
104
1101A
1101B
1101C
サーバ
1104
1102A
1102B
1102C

【図１２】

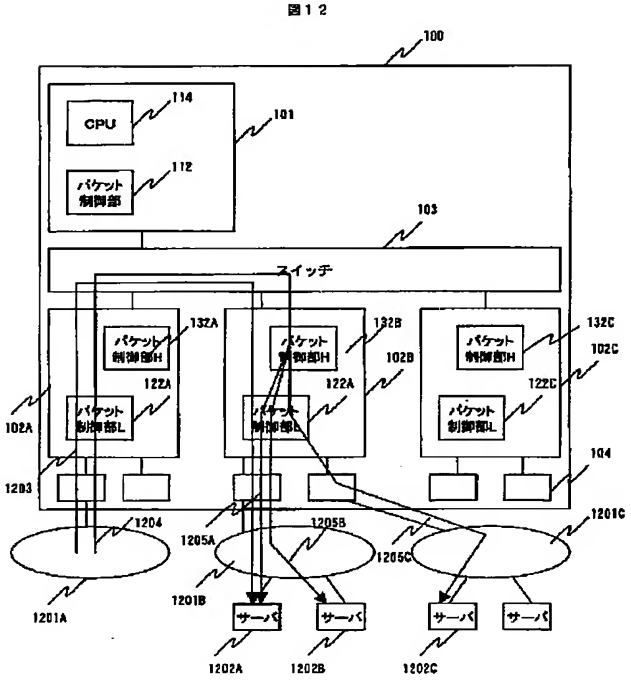
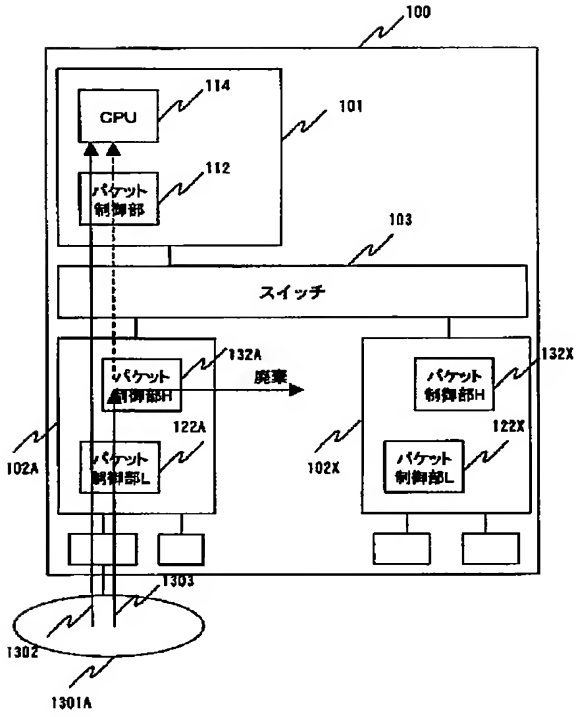


図１２
100
CPU
114
101
パケット制御部
112
103
スイッチ
パケット制御部H
132A
132B
132C
102C
102B
パケット制御部L
122A
122C
102A
1203
104
1204
1205A
1205B
1205C
1201C
1201A
1201B
サーバ
1202A
1202B
1202C

【図１３】

図１３



【図１４】

図１４